SPYWOLF

Security Audit Report

Completed on

July 1, 2022

MADE IN USA 🇺🇸

OVERVIEW

This audit has been prepared for **The Boys Token** to review the main aspects of the project to help investors make make an informative decision during their research process.

You will find a a summarized review of the following key points:

- ✔ Contract's source code
- ✔ Owners' wallets
- ✔ Tokenomics
- ✔ Team transparency and goals
- ✔ Website's age, code, security and UX
- ✔ Whitepaper and roadmap
- ✔ Social media & online presence

The results of this audit are purely based on the team's evaluation and does not guarantee nor reflect the projects outcome and goal

- SPYWOLF Team -

TABLE OF CONTENTS

The Boys Token

PROJECT DESCRIPTION

According to their website:

The Boys Token project will be riding the hype around the Amazon Prime Video Tv Series " The Boys ".

Project's Priority is building a strong community in the BSC space and leading the token from BSC to other networks.

Future developments of the project:

- **Exclusive NFTs with Rarities**
- **Token Staking & NFTs Staking**
- **NFT Mortal Kombat Game Type "The Boys Game (Fight to earn)**

Release Date: Launched on June 30, 2022

Category:

CONTRACT INFO

Token Name
The Boys Token

Symbol
BOYS

Contract Address
0x5c1F9A9dF35a4E57f971af06F5F98Dfe21Cfccd5

Network
Binance Smart Chain

Language
Solidity

Deployment Date
June 30, 2022

Verified?
Yes

Total Supply
10,000,000

Status
Launched

TAXES

Buy Tax
10%

Sell Tax
10%

*Taxes can be changed in future

Our Contract Review Process

The contract review process pays special attention to the following:

- Testing the smart contracts against both common and uncommon vulnerabilities
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Ensuring contract logic meets the specifications and intentions of the client.
- Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- Thorough line-by-line manual review of the entire codebase by industry experts.

Blockchain security tools used:

- OpenZeppelin
- Mythril
- Solidity Compiler
- Hardhat

CURRENT STATS

(AS OF June 1, 2022)

Status:
Launched!

Liquidity

PancakeSwap:
74 WBNB

Burn

10% of total supply

MaxTxAmount
100,000

DEX:
PancakeSwap

LP Address(es)

PancakeSwap:
0xEF8157E3060ACD7d04f035630698F086e7e5821c

93.93% locked in PinkLock - unlocks at 2022.08.31
https://www.pinksale.finance/pinklock/record/1012991?chain=BSC

Locked wallets

0x2BAe54fD83806d44afdBA35BF1A210daCaF36b72

20% ot total supply locked in PinkLock - unlocks at 2022.08.31
https://www.pinksale.finance/pinklock/record/1012990?chain=BSC

TOKEN TRANSFERS STATS

Transfer Count	3083
Uniq Senders	468
Uniq Receivers	769
Total Amount	27269080 BOYS
Median Transfer Amount	820 BOYS
Average Transfer Amount	8844 BOYS
First transfer date	2022-06-30
Last transfer date	2022-07-01
Days token transferred	2

SMART CONTRACT STATS

Calls Count	5550
External calls	732
Internal calls	4818
Transactions count	2107
Uniq Callers	719
Days contract called	2
Last transaction time	2022-07-01 08:22:43
Created	2022-06-30 08:43:27
Create TX	0x43166757a286849e9a13ecc01399282c0736551590f144be69d6f32eaa4377b2
Creator	0x2bae54fd83806d44afdba35bf1a210dacaf36b72

FEATURED WALLETS

Owner address	0x2bae54fd83806d44afdba35bf1a210dacaf36b72
Dev wallet	0x75c2d282cc01d06ac5dc324878fea28246d1acc0
Marketer wallet	0x46Bd3c9F6ba99331FDb067DdcEaB6411B5631478
Marketing wallet	0xe7aa54b7376afea3ba3132ff266b6c789d922f92
Team wallet	0x498885ed421a2cce5c3ca2f69cdc97af5a70f1f4
Utility wallet	Same as owner
LP address	0xEF8157E3060ACD7d04f035630698F086e7e5821c **93.93% locked in PinkLock - unlocks at 2022.08.31**

TOP 3 UNLOCKED WALLETS

1 17.89% ⚠️Same as owner

2 1.15% 0x85cef64550532fdbd8015133631bfdf5d47f144a

3 0.45% 0xdda19c5edd0b230933f75e24fc04479d2dfc7ce8

VULNERABILITY CHECK

Design Logic	Passed
Compiler warnings.	Passed
Private user data leaks	Passed
Timestamp dependence	Passed
Integer overflow and underflow	Passed
Race conditions and reentrancy. Cross-function race conditions	Passed
Possible delays in data delivery	Passed
Oracle calls	Passed
Front running	Passed
DoS with Revert	Passed
DoS with block gas limit	Passed
Methods execution permissions	Passed
Economy model	Passed
Impact of the exchange rate on the logic	Passed
Malicious Event log	Passed
Scoping and declarations	Passed
Uninitialized storage pointers	Passed
Arithmetic accuracy	Passed
Cross-function race conditions	Passed
Safe Zeppelin module	Passed
Fallback function security	Passed

THREAT LEVELS

When performing smart contract audits, our specialists look for known vulnerabilities as well as logical and access control issues within the code. The exploitation of these issues by malicious actors may cause serious financial damage to projects that failed to get an audit in time. We categorize these vulnerabilities by the following levels:

High Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Medium Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Low Risk

Issues on this level are minor details and warning that can remain unfixed.

Informational

Information level is to offer suggestions for improvement of efficacy or security for features with a risk free factor.

FOUND THREATS

⚠ High Risk

Owner can withdraw tokens from any address, including liquidity pair and locking contracts.
Once the 'tradingStatus_launchmode' function is executed, the owner won't be able withdraw tokens from non blacklisted addresses.
The 'tradingStatus_launchmode' function is currently not executed.

```
function multiTransfer(address from, address[] calldata addresses,
 uint256[] calldata tokens) external authorized {
    if(msg.sender != from && !isBlacklisted[from]){
        require(launchMode,"Cannot execute this after launch is done");
    }
    require(addresses.length < 501,"GAS Error: max limit is 500 addresses");
    require(addresses.length == tokens.length,"Mismatch between address and token count");
    uint256 SCCC = 0;
    for(uint i=0; i < addresses.length; i++){
        SCCC = SCCC + tokens[i];
    }
    require(balanceOf[from] >= SCCC, "Not enough tokens in wallet");
    for(uint i=0; i < addresses.length; i++){
        _basicTransfer(from,addresses[i],tokens[i]);
    }
}

function tradingStatus_launchmode(uint256 confirm) external onlyOwner {
    require(confirm == 911911911,"Accidental Press"); // just paranoid
    require(tradingOpen,"Cant close launch mode when trading is disabled");
    require(!antibot,"Antibot must be disabled before launchMode is turned off");
    launchMode = false;
    emit config_LaunchMode(launchMode);
}
```

FOUND THREATS

⚠ High Risk

Owner can blacklist address, making it impossible to sell until the 'tradingStatus_launchmode' function is triggered.
Once the 'tradingStatus_launchmode' function is executed, the owner won't be able to blacklist address.
The 'tradingStatus_launchmode' function is currently not executed.

```
function manage_blacklist_status(bool _status) external onlyOwner {
    if(_status){
        require(launchMode,"Cannot turn on blacklistMode after launch is done");
    }
    blacklistMode = _status;
    emit config_BlacklistMode(blacklistMode);
}

function manage_blacklist(address[] calldata addresses, bool status) external onlyOwner {
    require(addresses.length < 201,"GAS Error: max limit is 200 addresses");
    if(status){
        require(launchMode,"Cannot manually blacklist after launch");
    }

    for (uint256 i=0; i < addresses.length; ++i) {
        blacklist_wallet(addresses[i],status);
    }
}

function tradingStatus_launchmode(uint256 confirm) external onlyOwner {
    require(confirm == 911911911,"Accidental Press"); // just paranoid
    require(tradingOpen,"Cant close launch mode when trading is disabled");
    require(!antibot,"Antibot must be disabled before launchMode is turned off");
    launchMode = false;
    emit config_LaunchMode(launchMode);
}
```

FOUND THREATS

⚠ High Risk

Owner can disable trading, making it impossible to sell until the 'tradingStatus_launchmode' function is triggered.
Once the 'tradingStatus_launchmode' function is executed, the owner won't be able to disable trading.
The 'tradingStatus_launchmode' function is currently not executed.

```
function tradingStatus(bool _status, bool _ab) external onlyOwner {
    if(!_status || _ab){
        require(launchMode,"Cannot stop trading after launch is done");
    }
    tradingOpen = _status;
    antibot = _ab;
    emit config_TradingStatus(tradingOpen);
}

function tradingStatus_launchmode(uint256 confirm) external onlyOwner {
    require(confirm == 911911911,"Accidental Press"); // just paranoid
    require(tradingOpen,"Cant close launch mode when trading is disabled");
    require(!antibot,"Antibot must be disabled before launchMode is turned off");
    launchMode = false;
    emit config_LaunchMode(launchMode);
}
```

FOUND THREATS

⚠ Medium Risk

Owner can change buy fees up to 15%, sell fees up to 24%, transfer fees up to 10%. Combined buy+sell = 39%.

```
function setFees_base1000(uint256 _liquidityFee,  uint256 _marketingFee,
uint256 _teamFee, uint256 _marketerFee, uint256 _utilityFee) external onlyOwner {
    liquidityFee = _liquidityFee;
    marketingFee = _marketingFee;
    teamFee = _teamFee;
    marketerFee = _marketerFee;
    utilityFee = _utilityFee;
    totalFee = _liquidityFee + _marketingFee + _teamFee + devFee + _utilityFee + _marketerFee;

    update_fees();
}

function update_fees() internal {
    require(totalFee.mul(buyMultiplier).div(100) <= 150, "Buy tax cannot be more than 15%");
    require(totalFee.mul(sellMultiplier).div(100) <= 240, "Sell tax cannot be more than 24%");
    require(totalFee.mul(transferMultiplier).div(100) <= 100, "Transfer Tax cannot be more than 10%");

    emit UpdateFee( uint8(totalFee.mul(buyMultiplier).div(100)),
        uint8(totalFee.mul(sellMultiplier).div(100)),
        uint8(totalFee.mul(transferMultiplier).div(100))
        );
}

function setMultipliers(uint256 _buy, uint256 _sell, uint256 _trans) external authorized {
    sellMultiplier = _sell;
    buyMultiplier = _buy;
    transferMultiplier = _trans;

    update_fees();
}
```

- Recommendation:
  - Considered as good tax deduction practice is buy and sell fees combined not to exceed 25%.

Informational

Owner can set max transaction limit, but can't lower it than 0.1% of total supply.

```
function setMaxTxPercent_base1000(uint256 maxTXPercentage_base1000) external onlyOwner {
    require(maxTXPercentage_base1000 >= 1,"Cannot set max transaction less than 0.1%");
    _maxTxAmount = (totalSupply * maxTXPercentage_base1000 ) / 1000;
    emit config_MaxTransaction(_maxTxAmount);
}
```

Owner can withdraw any tokens from the contract.

```
function clearStuckBalance(uint256 amountPercentage) external onlyOwner {
    require(amountPercentage < 101, "Max 100%");
    uint256 amountBNB = address(this).balance;
    uint256 amountToClear = ( amountBNB * amountPercentage ) / 100;
    payable(msg.sender).transfer(amountToClear);
    emit BalanceClear(amountToClear);
}

function clearStuckToken(address tokenAddress, uint256 tokens) external onlyOwner returns (bool success) {
    if(tokens == 0){
        tokens = BEP20(tokenAddress).balanceOf(address(this));
    }

    emit clearToken(tokenAddress, tokens);

    return BEP20(tokenAddress).transfer(msg.sender, tokens);
}
```

RECOMMENDATIONS FOR

GOOD PRACTICES

1. Consider fundamental tradeoffs
2. Be attentive to blockchain properties
3. Ensure careful rollouts
4. Keep contracts simple
5. Stay up to date and track development

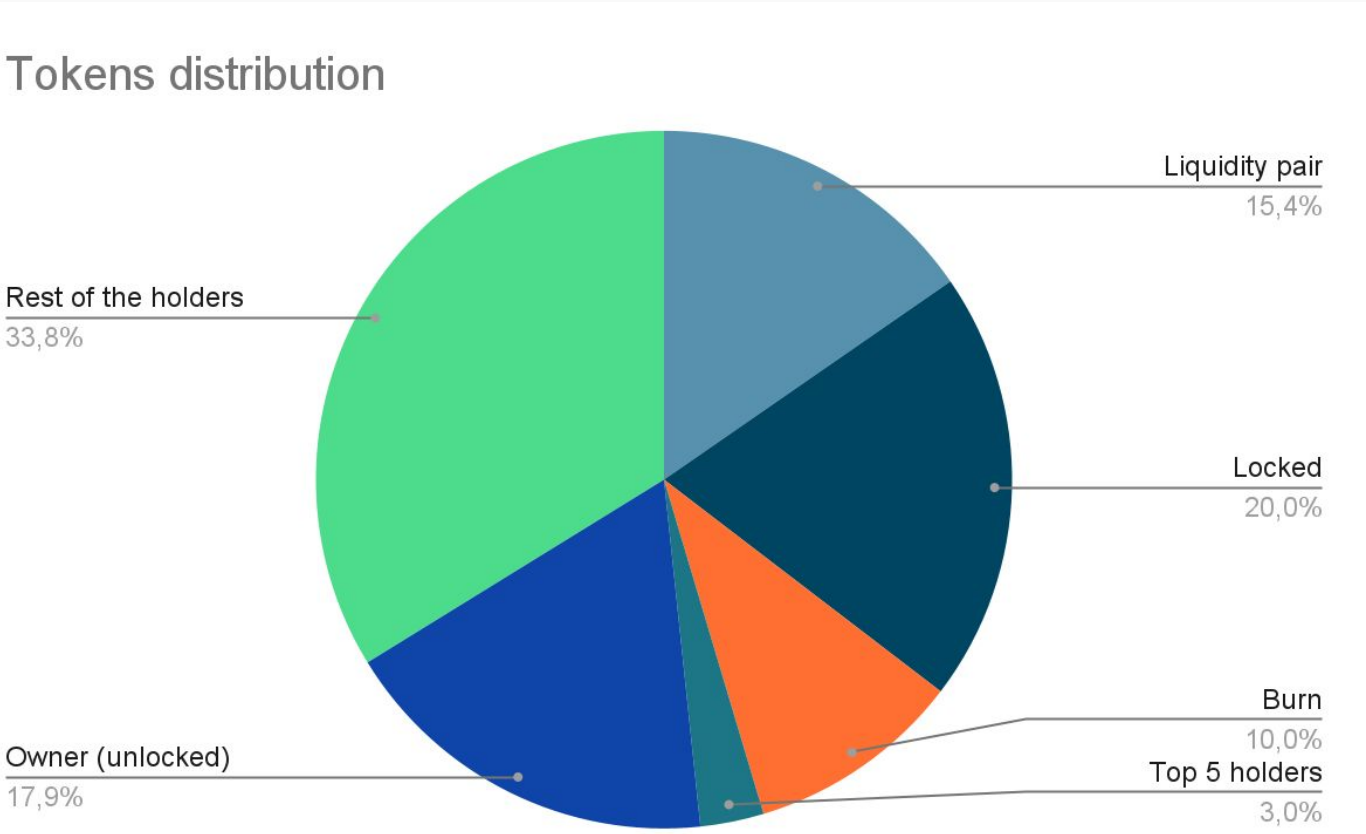
The Boys Token

GOOD PRACTICES FOUND

- ✔ The owner cannot mint new tokens after deployment
- ✔ The owner can set a transaction limit, but can’t lower it than 0.1% of total supply
- ✔ The smart contract utilizes "SafeMath" to prevent overflows

Current state:

- 15.38% - Liquidity pair
- 20% - Locked
- 10% - Burn
- 2.95% - Top 5 holders
- 17.89% - Owner (⚠️unlocked)
- 33.78% - Rest of the holders



TOKENOMICS

THE TEAM

The team has privately doxxed to SPYWOLF by completing the following KYC requirements:

- ID Verification
- Video statement
- Video interview with devs
- Owner's wallet verification

KYC INFORMATION

Issuer

SPYWOLF

Members KYC'd

KYC Date

July 01, 2022

Format

Image

Certificate Link

https://github.com/SpyWolfNetwork/KYCs/blob/main/june/KYC_THEBOYSTOKEN_0x5c1F9A9dF35a4E57f971af06F5F98Dfe21Cfccd5.png

WEBSITE

Website URL
https://theboystoken.finance/

Domain Registry
https://www.namecheap.com/

Domain Expiration
Expires on 2023-06-28

Technical SEO Test
Passed

Security Test
Passed. SSL certificate present

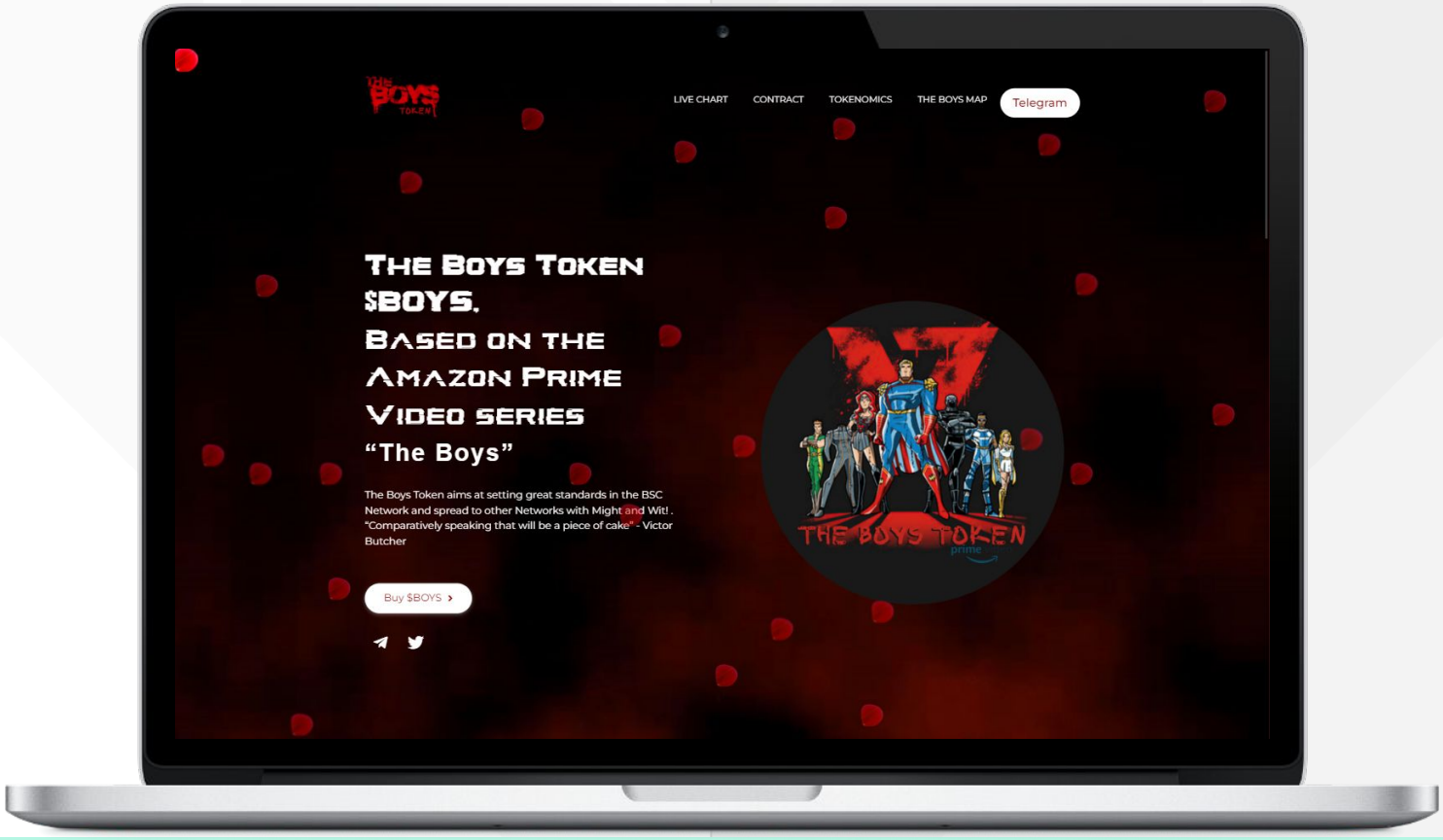
Design
Appropriate color scheme and graphics.

Content
Informative, no grammar mistakes found.

Whitepaper
⚠️ No whitepaper.

Roadmap
Yes, goals set at 3 phases without time frames.

Mobile-friendly?
Yes



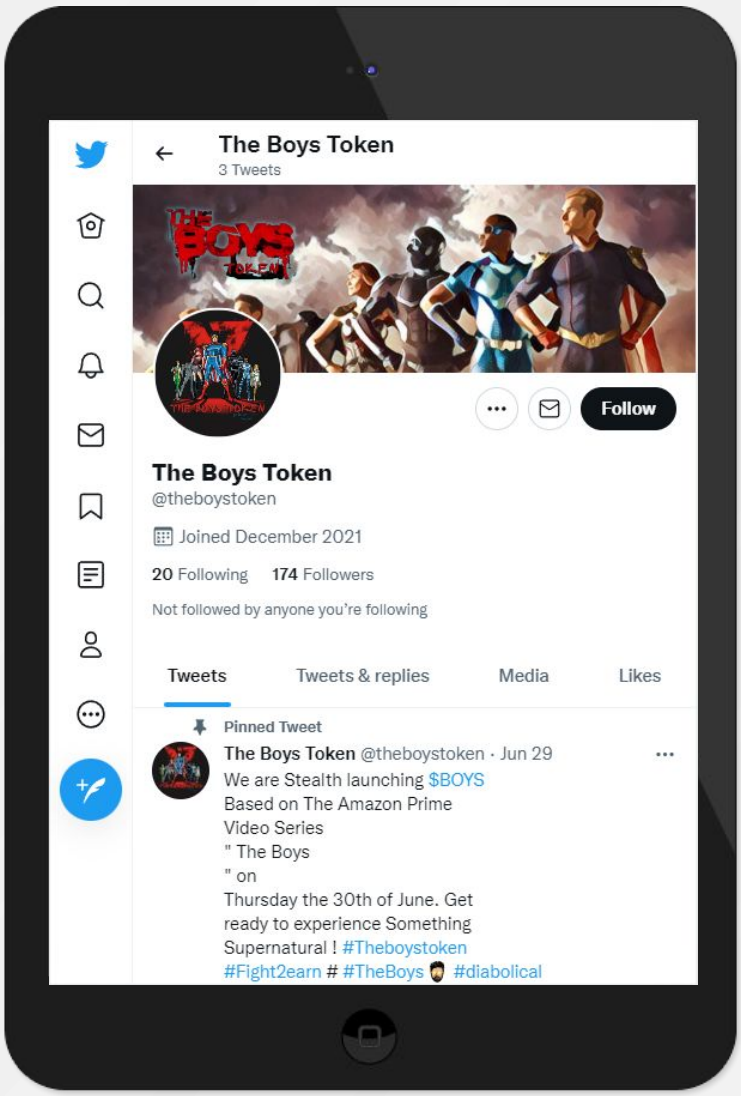
theboystoken.finance

SOCIAL MEDIA

& ONLINE PRESENCE

ANALYSIS

Project's social media presence is very recent (few days old). The mods are active, there are organic interactions on Telegram, but low activity on Twitter.



Twitter

@theboystoken

- 174 followers
- Recently active - 3 tweets, last one June 29
- Few active followers

Discord

Discord link here

- Not available

Telegram

@theboystoken

- 1391 members
- Active mods/team
- Organic interactions

Medium

Medium link here

- Not available

SPYWOLF

CRYPTO SECURITY

Audits | KYCs | dApps
Contract Development

ABOUT US

We are a growing crypto security agency offering audits, KYCs and consulting services for some of the top names in the crypto industry.

- **OVER 150 SUCCESSFUL CLIENTS**
- **MORE THAN 500 SCAMS EXPOSED**
- **MILLIONS SAVED IN POTENTIAL FRAUD**
- **PARTNERSHIPS WITH TOP LAUNCHPADS, INFLUENCERS AND CRYPTO PROJECTS**
- **CONSTANTLY BUILDING TOOLS TO HELP INVESTORS DO BETTER RESEARCH**

To hire us, reach out to
contact@spywolf.co or
t.me/joe_SpyWolf

FIND US ONLINE

SPYWOLF.CO

SPYWOLF.NETWORK

@SPYWOLFNETWORK

@SPYWOLFOFFICIAL

@SPYWOLFNETWORK

@SPYWOLFNETWORK

Disclaimer

This report shows findings based on our limited project analysis, following good industry practice from the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, overall social media and website presence and team transparency details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report.
While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the disclaimer below – please make sure to read it in full.

DISCLAIMER:
By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice.
No one shall have any right to rely on the report or its contents, and SpyWolf and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (SpyWolf) owe no duty of care towards you or any other person, nor does SpyWolf make any warranty or representation to any person on the accuracy or completeness of the report.
The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and SpyWolf hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, SpyWolf hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against SpyWolf, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report. The analysis of the security is purely based on the smart contracts, website, social media and team.
No applications were reviewed for security. No product code has been reviewed.